学校编码：10384
学号：23320061152607
分类号_____密级_____
UDC _____

厦门大学

硕 士 学 位 论 文

嵌入式 CPU 指令系统通用仿真研究与实现

The Research and Implementation Of Universal Simulation In Embedded CPU Instruction System

黄南戈

指导教师姓名： 林聪仁 副教授
专 业 名 称： 通信与信息系统
论文提交时间： 2009 年 5 月
论文答辩日期： 2009 年 月
学位授予日期： 2009 年 月

答辩委员会主席_____
评 阅 人_____

2009 年 5 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

2009　年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

2009 年　　月　　日

摘要

嵌入式系统的软件仿真可以使开发者对嵌入式系统架构的正确性及性能进行验证，从而大大降低开发成本和时间，是保证和提高嵌入式开发软件可靠性的重要手段。但目前市场上大多数的嵌入式系统软件仿真平台中对 CPU 指令模块的仿真都是从编译后的机器语言入手，这样就造成对嵌入式处理器生产厂家的编译器的依赖，阻碍了软件仿真的发展。为此本文提出了基于源代码分析的指令仿真技术，即对嵌入式应用软件代码的仿真采取直接从汇编源代码仿真执行入手，而不需要通过具体的机器语言，并提出用基于编译原理的“三个分析”方法来实现对源代码的功能仿真。

在目前现有的嵌入式系统软件仿真工具中，还未出现针对凌阳 SPCE061A 单片机的软件仿真器。另外在主流软件仿真器中，也主要是对某一款具体处理器型号的单一仿真，还未做到嵌入式系统软件仿真平台的通用。针对这种情况，本文基于凌阳 SPCE061A 处理器对 CPU 的运行原理和仿真实现方法进行了探索性的研究，目的是找出针对不同 CPU 结构的通用仿真方法。

本文初步实现了基于 SPCE061A 的通用嵌入式软件指令仿真工具 USMIC，该工具主要是以基于面向对象技术的 Visual C++6.0 为开发工具，其功能主要实现对开发者按照汇编语法规则输入的汇编源程序进行识别、仿真执行并给出仿真结果，仿真的整个过程均在可视化窗口中实现。对 USMIC 工具进行的初步测试结果表明 USMIC 工具已基本实现对凌阳 SPCE061A 汇编源程序的功能性仿真。

关键词： 指令仿真；通用仿真；源代码仿真

Abstract

Software simulation is used to test the validity and performance of the structure in embedded system, which greatly reduces the cost and time of development. In addition, it's an important method to guarantee and improve the reliability of embedded developing software. But at present, most of the software simulation platform for simulating CPU module in embedded system is based on the binary code after compiling, which causes the dependence to the compiler of specific microcontrollers, and hinders the development of software simulation. This thesis proposes an instruction simulation method based on the source code. In this way, the simulation of embedded application software code is directly taken from the assembly code, but not from specific machine language. This thesis also proposes the "three analysis "method based on the principle of compiling.

Among the software simulation tools in embedded system, there is still short of the sunplus SPCE061A microprocessor simulation software. And mainstream simulators are mainly used for a specific type processor, still lacking universal software simulation platform in embedded system. In view of this situation, and based on the sunplus SPCE061A microprocessor, this thesis has done a lot of work to search after the functional principle of CPU and the method of simulation ,and to find out the universal simulation method to kinds of CPUs.

This thesis has primarily realized the universal embedded software simulation tools USMIC based on SPCE061A, and it mainly uses Visual c++ 6.0 which is based on object-oriented technology as development tools. USMIC's main function is to identify the source code, execute it, and then put out the simulation results, right after the developer puts in the assembly source code in accordance with grammatical rules. The whole process of simulation can be monitored in visual window. The preliminary test of USMIC tool shows that USMIC has realized functional simulation of assembly source code of sunplus SPCE061A.

Key Words: Instruction Simulation; Universal Simulation; Simulation Based On Source Code.

目录

Contents

第一章 绪论

1.1 课题研究背景

1.1.1 软件可靠性

随着计算机技术和软件技术的飞速发展，软件可靠性已成为软件技术发展的突出问题。对于软件而言,可靠性是一个非常重要的性能指标,对于嵌入式软件来说尤为如此。在水声通信领域中的嵌入式应用系统，由于水下工作环境的特殊性、恶劣性，其可靠性方面的要求更高。而在其他通信领域的嵌入式系统中，同样需要可靠性的保障。

1983 年美国 IEEE 计算机学会对“软件可靠性”作出了明确定义，此后该定义被美国标准化研究所接受为国家标准，1989 年我国也接受该定义为国家标准。该定义包括两方面的含义：

1．在规定的条件下，在规定的时间内，软件不引起系统失效的概率；

2．在规定的时间周期内，在所述条件下程序执行所要求的功能的能力；

其中的概率是系统输入和系统使用的函数，也是软件中存在的故障的函数，系统输入将确定是否会遇到已存在的故障（如果故障存在的话）[1]。

目前由于软件可靠性不足的问题已经在全球范围内的各个领域带来了许多重大的损失。如美国 IBM 公司开发 OS/360[2]系统耗掉大量人力财力后，在后期仍然发现了上千个错误。美国放射治疗仪由使用机械安全互锁装置的 Therac 6 改进到使用软件安全互锁装置的 Therac 25 型后，故障率也由零演变到造成了两人死亡和多人受伤的重大医疗事故。海湾战争中 F/A－18 飞机飞行控制系统计算机 500 次故障中，软件故障次数超过硬件。90 年代后半期,“千年虫”问题震惊世界,各国投入了大量的人力和物力,耗资数千亿美元,虫害才基本上得到控制。“千年虫”实际上就是一种特殊的软件故障[3]。

由此可见，提高软件的可靠性以成为软件发展的突出问题。这就要求在大力发展软件开发技术的同时，需要高度重视和提高软件可靠性的问题。

国际上软件可靠性问题获得重视是在 20 世纪 60 年代末期，那时软件危机被广泛讨论，软件不可靠是造成软件危机的重要原因之一。国外从那时候开始

研究并提出了多种可靠性模型和预测方法，如 1972 年提出的 Jelinski—Moranda 模型[4]，标志着软件可靠性系统研究的开始。在 80 年代，软件可靠性从研究阶段逐渐迈向工程化。并于 90 年前后形成较为系统的软件可靠性体系[3]。目前国际上软件可靠性发展比较有影响的学术会议有：软件保证、确认国际会议（ISACC)、软件维护国际会议（ISSM）和软件可靠性工程国际会议（ISSRE）等。

国内对可靠性的研究同样始于上世纪 60 年代，但起初主要集中在电子元器件的可靠性标准上，对软件可靠性的重视不够。而软件可靠性研究则始于 80 年代初，主要代表有：黄锡滋在软件的可靠性设计、软件测试、软件可靠性预计模型、软件与硬-软件复合系统结构模型、软件系统安全性分析、程序的复杂性与可靠性分配、软件维护、软件的质量保证等方面作了有益的探索[5]；徐仁佐在软件可靠性建模等方面做了有益的探索[6]。姚一平等在软件可靠性建模、软件可靠性评估工具和混合硬件-软件系统可靠性等方面作了努力[7]；蔡开元在软件可靠性分析、测试与评估工具，软件控制论在可靠性中的运用和构件软件系统可靠性评估模型等方面作了有益的探讨[8]。

自从 1992 年以来,我国在软件可靠性方面的基础理论研究与国外十分接近,但在工程应用、度量标准（指标体系)、建模技术、设计方法、测试技术等方面却有相当大的差距。如今，随着二十一世纪以来中国在世界软件业地位上的巨大提升，亟待在软件可靠性方面的研究。国家为了推动这方面的研究，提供了很多项目资助，如 2007 年国家自然科学基金委员会启动“可信软件基础研究”重大研究计划等[9]。

1.1.2 系统仿真

仿真是指在实际系统尚不存在的情况下对于系统或活动本质的实现，这是 G.W.Morgenthater 于 1961 年首次对“仿真”进行的技术性定义。现代仿真技术均是在计算机的支持下进行的，因而，系统仿真也称为计算机仿真[10]。

在系统仿真中，用软件仿真的方式一直是一个重要的研究领域。在构建一个新系统时，有效地测试和验证新系统的行为和正确性十分重要。软件仿真是通过软件的执行来模拟硬件行为的一种方法。软件仿真器是在宿主机上运行并